Remarks/Arguments

The Applicants respectfully request further examination and reconsideration in view of the amendments made above and the comments set forth below. Claims 1-45, 47-52, and 59-71 were pending. Claims 46 and 53-58 were previously canceled. Within the Office Action, Claims 16, 40, 59, and 60 have been rejected under 35 U.S.C. § 112, second paragraph; and Claims 1-45, 47-52, and 59-69 have been rejected under 35 U.S.C. § 103(a). By way of the amendments made above, Claims 1, 16, 26, 36, 40, 48, 59, 60, 70, and 71 have been amended. Accordingly, Claims 1-45, 47-52 and 59-71 are now pending.

Rejections under 35 U.S.C. § 112, second paragraph

Within the Office Action, Claims 16, 40, 59, and 60 are rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that the Applicants regard as their invention. Specifically, it is stated, "As to claims 16, 40, 70, and 71, it is unclear from the language whether an encryption key or an **encrypted** encryption key is used for the encryption of the file name and the file contents" (bold in original).

An encryption key can be encrypted and then used as input to generate other types of data. An encryption key for encrypting one type of data cannot first be encrypted and then used to encrypt that same type of data. That encryption key can, however, be used to encrypt the data, be encrypted itself, and then used as a key or other input for encrypting another type of data. As explained below, some of the claims recite that a key used to encrypt a file name (one type of data) is used together with file contents (another type of data) to generate encrypted file contents.

By way of the above amendments, Claims 16, 40, 70, and 71 have all been amended to more clearly define the invention. Claim 16 has been amended to recite encrypting data file contents with an *encrypting* data file contents key and *encrypting* a data file name with an encrypting data file name key. Accordingly, the rejection of Claim 16 under 35 U.S.C. § 112, second paragraph, is now moot.

Claim 40 recites "processing the file contents together with the encrypted data file name key to generate an encrypted file contents key and an encrypted file contents." This limitation is clear: A key used to encrypt a file name can be encrypted and used to encrypt file contents. In other words, an encrypted key can be used (*e.g.*, as an input to an algorithm) to generate any number of other keys for encrypting other types of data. Such methods add added layers of

security to encrypting kernels. Accordingly, the rejection of Claim 40 under 35 U.S.C. § 112, second paragraph, is now moot. This limitation finds support in the Specification, at page 21, lines 3-13.

Claim 70 has been amended to recite "encrypt the file contents with an *encrypting* file contents key to generate encrypted file contents"; and Claim 70 has been amended to recite, "processing the file contents together with the *encrypted* file name key to generate an encrypted file contents key and encrypted file contents" (italics added to both claims). Claims 70 and 71 no longer recite using an encrypted key to encrypt anything. Like Claim 40, Claim 70 now clearly recites that an encrypted file name key is used, such as one input to an algorithm, to generate other encrypted data. Accordingly, the rejections of Claims 70 and 71 under 35 U.S.C. § 112, second paragraph, are now moot.

It is stated within the Office Action, "As to Claim 59, it appears the limitations of the claims are method steps and not part of the system of base claim 1. The Examiner will interpret the limitations as the system configured to." In response to this interpretation, Claim 59 has been amended to recite a limitation corresponding to this interpretation: "wherein the kernel is further configured to encrypt or decrypt a data file in the directory with a corresponding file encryption key and to encrypt or decrypt the directory with a directory encryption key." Accordingly, the rejection of Claim 59 is now moot.

It is stated within the Office Action, "As to Claim 60, the limitations refer to a plurality of file encryption keys, but there [is] only one file encryption key in the parent claims and is therefore, unclear." Claim 59, from which Claim 60 depends, has been amended to recite, "a corresponding one of multiple file encryption keys." Accordingly, there is sufficient antecedent basis for the recitation of "the multiple file encryption keys" in Claim 60. Accordingly, the rejection of Claim 60 is now moot.

Rejections under 35 U.S.C. § 103(a)

Claims 1-5, 9, 12, 19, 20, 26-28, 31, 36, 37, 42, 43, 48-50, and 61-69

Within the Office Action, Claims 1-5, 9, 12, 19, 20, 26-28, 31, 36, 37, 42, 43, 48-50, and 61-69 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,313,694 to Riedel ("Riedel") in view of Zadok, "Cryptfs: A Stackable Vnode Level Encryption File System" ("Zadok"). The Applicants respectfully disagree.

Riedel is directed to a technique for secure file access control via directory encryption. Riedel discloses encrypting filenames to protect them in the event a server is untrustworthy, such as in a distributed computing environment. Riedel also discloses encrypting filenames in a directory structure without otherwise changing the directory structure. (Riedel, Abstract)

Zadok discloses a "stackable" vnode interface. As Zadok explains in its section 1.1, "With vnode stacking, several vnode interfaces may exist and may call each other in sequence: the code for a certain operation at stack level N typically calls the corresponding operation at level N-1, and so on." Zadok further explains: "Cryptfs is designed to be simple in principle. The file system interposes (mounts) itself on top of any directory, encrypts file data before it is passed to the interposed-upon file system, and decrypts in the reverse direction." (Zadok, page 2, col. 2, first full paragraph) As shown in Figure 1 of Zadok, the Cryptfs layer is separate from the vnode layer; it is a separate module whose encryption components are not integrated with the vnode layer. Cryptfs is modular file system that is mounted in the kernel but is not integrated with the vnode. Cryptfs is a feature inside a kernel that works with low level functions of the kernel to provide the Cryptfs file system.

In contrast, in accordance with the present invention, a virtual memory facility is modified so that all incoming data is decrypted and all outgoing data is encrypted: a vnode in accordance with the present invention is modified to encrypt and decrypt data entering and leaving kernel space. In one embodiment, "encryption drivers are integrated into the vnode interface structure" of UNIX source code. (Specification at page 45, lines 17-18; see also page 59, lines 24-25)

As further differences, Cryptfs uses user sessions to protect against cloning user IDs (UIDs), whereas embodiments of the present invention use i-node information such as the credentials of a user, which may or may not include UIDs.

The independent Claim 1 is directed to a computer system comprising a memory portion containing an encrypted data file and an operating system comprising a kernel. The kernel of Claim 1 comprises a virtual node configured to decrypt an encrypted directory entry to determine a location of the encrypted data file and to decrypt the encrypted data file to access data contained therein. Neither Riedel nor Zadok, either alone or in combination, discloses a virtual node configured to decrypt an encrypted directory entry to determine a location of the encrypted data file and to decrypt the encrypted data file to access data contained therein, as recited in Claim 1. For at least these reasons, the independent Claim 1 is allowable over Riedel, Zadok, and their combination.

Claims 2-5, 9, 12, 19, 20, 61, and 62 all depend on the independent Claim 1. As explained above, the independent Claim 1 is allowable over Riedel, Zadok, and their combination. Accordingly, Claims 2-5, 9, 12, 19, 20, 61, and 62 are all also allowable as depending on an allowable base claim.

The independent Claim 26 is directed to a computer system comprising a first device and a second device. The first device has an operating system kernel and a directory structure with directory information comprising encrypted data file names and corresponding encrypted data file locations for accessing encrypted data files within a file system. The operating system kernel is configured to decrypt the encrypted data file names and encrypted data file locations using one or more encryption keys to recover clear data corresponding to the data file names, data file locations, and data files. The operating system kernel comprises a virtual node configured to encrypt the clear data using the one or more encryption keys to generate cipher data corresponding to the directory information and encrypted data files. The second device is coupled to the first device and is configured to exchange cipher data with the first device. Neither Riedel nor Zadok, either alone or in combination, discloses an operating system kernel that comprises a virtual node configured to encrypt the clear data using the one or more encryption keys to generate cipher data corresponding to the directory information and encrypted data files, as recited in Claim 26. For at least these reasons, the independent Claim 26 is allowable over Riedel, Zadok, and their combination.

Claims 27, 28, 31, and 63-65 all depend on the independent Claim 26. As explained above, the independent Claim 26 is allowable over Riedel, Zadok, and their combination. Accordingly, Claims 27, 28, 31, and 63-65 are all also allowable as depending on an allowable base claim.

The independent Claim 36 is directed to a method of storing an encrypted data file in a computer file system having a directory. The method of Claim 36 comprises receiving a clear data file having a name and executing kernel code in an operating system, the kernel code comprising a virtual node integrated with drivers configured to encrypt the clear data file to generate an encrypted data file using a symmetric key, store the encrypted data file at a location in the computer file system, and store in the directory an entry containing an encryption of the name and an encryption of the location. Neither Riedel nor Zadok, either alone or in combination, discloses kernel code that comprises a virtual node integrated with drivers configured to encrypt the clear data file to generate an encrypted data file using a symmetric key, store the encrypted data file at a location in the computer file system, and store in the directory an

entry containing an encryption of the name and an encryption of the location, as recited in Claim 36. For at least these reasons, the independent Claim 36 is allowable over Riedel, Zadok, and their combination.

Claims 37, 42, 43, 66, and 67 all depend on the independent Claim 36. As explained above, the independent Claim 36 is allowable over Riedel, Zadok, and their combination. Accordingly, Claims 37, 42, 43, 66, and 67 are all also allowable as depending on an allowable base claim.

The independent Claim 48 is directed to a computer system that comprises a processor, a physical memory containing an encrypted data file and a directory, a secondary device coupled to the physical memory, and an operating system comprising a kernel. The directory comprises a record having a first element corresponding to an encrypted name of the data file and a second element corresponding to an encrypted location of the data file in the memory. The kernel comprises a virtual node integrated with drivers configured to decrypt the first and second elements to access the encrypted data file from memory when transferring the data file from the memory to the secondary device and to re-encrypt the first and second elements when transferring the data file from the secondary device to the memory. Neither Riedel nor Zadok, either alone or in combination, discloses a kernel that comprises a virtual node integrated with drivers configured to decrypt the first and second elements to access the encrypted data file from memory when transferring the data file from the memory to the secondary device and to re-encrypt the first and second elements when transferring the data file from the secondary device to the memory, as recited in Claim 48. For at least these reasons, the independent Claim 48 is allowable over Riedel, Zadok, and their combination.

Claims 49, 50, 68, and 69 all depend on the independent Claim 48. As explained above, the independent Claim 48 is allowable over Riedel, Zadok, and their combination. Accordingly, Claims 49, 50, 68, and 69 are both also allowable as depending on an allowable base claim.

Claims 6-8, 11, 14, 15, 29, 38, 39, 51, and 52

Within the Office Action, Claims 6-8, 11, 14, 15, 29, 38, 39, 51, and 52 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Riedel in view of Zadok as applied to claim 1, and further in view of U.S. Patent Pub. No. 2003/0005300 to Noble et al. ("Noble"). The Applicants respectfully disagree.

Claims 6-8, 11, 14, and 15 all depend on the independent Claim 1. As explained above, the independent Claim 1 is allowable. Accordingly, Claims 6-8, 11, 14, and 15 are all also allowable as depending on an allowable base claim.

Claim 29 depends on the independent Claim 26. As explained above, the independent Claim 26 is allowable. Accordingly, Claim 29 is also allowable as depending on an allowable base claim.

Claims 38 and 39 both depend on the independent Claim 36. As explained above, the independent Claim 36 is allowable. Accordingly, Claims 38 and 39 are both also allowable as depending on an allowable base claim.

Claims 51 and 52 both depend on the independent Claim 48. As explained above, the independent Claim 48 is allowable. Accordingly, Claims 51 and 52 are both also allowable as depending on an allowable base claim.

Claims 10 and 30

Within the Office Action, Claims 10 and 30 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Riedel in view of Zadok, and further in view of Noble as applied to Claim 5, and further in view of U.S. Patent No. 5,903,881 to Schrader et al. ("Schrader"). The Applicants respectfully disagree.

Claim 10 depends on the independent Claim 1. As explained above, the independent Claim 1 is allowable. Accordingly, Claim 10 is also allowable as depending on an allowable base claim.

Claim 30 depends on the independent Claim 26. As explained above, the independent Claim 26 is allowable. Accordingly, Claim 30 is also allowable as depending on an allowable base claim.

Claim 13

Within the Office Action, Claim 13 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Riedel in view of Zadok as applied to Claim 12, and further in view of U.S. Patent No. 5,727,206 to Fish et al. ("Fish"). The Applicants respectfully disagree.

Claim 13 depends on the independent Claim 1. As explained above, the independent Claim 1 is allowable. Accordingly, Claim 13 is also allowable as depending on an allowable base claim.

Claims 16-18, 25, 40, 70, and 71

Within the Office Action, Claims 16-18, 25, 40, 70, and 71 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Riedel in view of Zadok as applied to Claim 15, and further in view of Blaze, "A Cryptographic File System for Unix" ("Blaze"). The Applicants respectfully disagree.

Claims 16-18 and 25 all depend on the independent Claim 1. As explained above, the independent Claim 1 is allowable. Accordingly, Claims 16-18 and 25 are also allowable as depending on an allowable base claim.

Claim 40 depends on the independent Claim 36. As explained above, the independent Claim 36 is allowable. Accordingly, Claim 40 is also allowable as depending on an allowable base claim.

Riedel and Zadok have been characterized above. Blaze is directed to a Cryptographic File System (CFS). Blaze discloses that "Users associate a cryptographic key with the directories they wish to protect. Files in these directories (as well as their pathname components) are transparently encrypted and decrypted with the specified key without further user intervention; cleartext is never stored on a disk or sent to a remote file server." (Blaze, Abstract) Blaze does not disclose an operating system kernel having a virtual node integrated with drivers to encrypt and decrypt data.

The independent Claim 70 is directed to a computer system containing an operating system. The computer system of Claim 70 comprises a kernel, a memory, and an encryption key management system. The kernel comprises a virtual node integrated with drivers configured to encrypt and decrypt data transferred between a memory and a secondary device. The kernel also comprises an encryption engine that is configured to encrypt clear data to generate cipher data. The encryption engine is also configured to decrypt the cipher data to generate the clear data. The memory is coupled to the encryption engine. The memory is configured to store the cipher data and comprises a first logical protected memory configured to store encrypted file data and a second logical protected memory configured to store encrypted key data. The encryption key management system is configured to control access to the encrypted file data and the encrypted key data. The encryption key management system comprises a key engine. The key engine is configured to receive a pass key and the file name to generate an encrypted file name key, use the encrypted file name key and file contents to generate an encrypted file contents key, and encrypt the file contents with an encrypting file contents key to generate encrypted file contents. Not one of Riedel, Zadok, and Blaze, either alone or in combination, discloses a kernel that comprises a

virtual node integrated with drivers configured to encrypt and decrypt data transferred between a memory and a secondary device. For at least these reasons, the independent Claim 70 is allowable over Riedel, Zadok, Blaze, and their combination

The independent Claim 71 is directed to a method of encrypting data. The method of Claim 71 comprises receiving clear data and executing kernel code in an operating system. The kernel code comprises a virtual node integrated with drivers configured to use a symmetric key to encrypt the clear data to generate cipher data and to use the symmetric key to decrypt the cipher data to generate the clear data. The executing the kernel code comprises entering a pass key and a file name into a first encryption process to produce an encrypted file name and an encrypted file name key and processing the file contents together with the encrypted file name key to generate an encrypted file contents key and encrypted file contents. Not one of Riedel, Zadok, and Blaze, either alone or in combination, discloses a kernel that comprises a virtual node integrated with drivers configured to use a symmetric key to encrypt clear data to generate cipher data and to use a symmetric key to decrypt cipher data to generate the clear data. For at least these reasons, the independent Claim 71 is allowable over Riedel, Zadok, Blaze, and their combination.

Claims 21, 32, and 44

Within the Office Action, Claims 21, 32, and 44 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Riedel in view of Zadok as applied to Claim 19, and further in view of U.S. Patent No. 6,836,888 to Basu et al. ("Basu"). The Applicants respectfully disagree.

Claim 21 depends on the independent Claim 1. As explained above, the independent Claim 1 is allowable. Accordingly, Claim 21 is also allowable as depending on an allowable base claim.

Claim 32 depends on the independent Claim 26. As explained above, the independent Claim 26 is allowable. Accordingly, Claim 32 is also allowable as depending on an allowable base claim.

Claim 44 depends on the independent Claim 36. As explained above, the independent Claim 36 is allowable. Accordingly, Claim 44 is also allowable as depending on an allowable base claim.

Claims 22-24, 33-35, 45, and 47

Within the Office Action, Claims 22-24, 33-35, 45, and 47 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Riedel in view of Zadok as applied to Claim 19, and

further in view of U.S. Patent No. 6,477,545 to LaRue ("LaRue"). The Applicants respectfully disagree.

Claims 22-24 all depend on the independent Claim 1. As explained above, the independent Claim 1 is allowable. Accordingly, Claims 22-24 are all also allowable as depending on an allowable base claim.

Claims 33-35, 45, and 47 all depend on the independent Claim 26. As explained above, the independent Claim 26 is allowable. Accordingly, Claims 33-35, 45, and 47 are all also allowable as depending on an allowable base claim.

Claim 41

Within the Office Action, Claim 41 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Riedel in view of Zadok as applied to Claim 40, and further in view of Noble. The Applicants respectfully disagree.

Claim 41 depends on the independent Claim 36. As explained above, the independent Claim 36 is allowable. Accordingly, Claim 41 is also allowable as depending on an allowable base claim.

Claims 59 and 60

Within the Office Action, Claims 59 and 60 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Riedel in view of Zadok as applied to Claim 1, and further in view of U.S. Patent No. 6,938,166 to Sarfati et al. ("Sarfati"). The Applicants respectfully disagree.

Claims 59 and 60 both depend on the independent Claim 1. As explained above, the independent Claim 1 is allowable. Accordingly, Claims 59 and 60 are both also allowable as depending on an allowable base claim.

CONCLUSION

For the reasons given above, the Applicants respectfully submit that Claims 1-45, 47-52 and 59-71 are in condition for allowance, and allowance at an early date would be appreciated. If the Examiner has any questions or comments, the Examiner is encouraged to call the undersigned at (408) 530-9700 so that any outstanding issues can be quickly and efficiently resolved.

Respectfully submitted,
HAVERSTOCK & OWENS LLP

Dated: December 22, 2008

By: /Jonathan O. Owens/
Jonathan O. Owens
Reg. No.: 37,902
Attorneys for Applicants